# UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

Apple IDs:kareemwarren602@icloud.com and kareemwarren0@icloud.com that is stored at premises controlled by Apple, Inc.

Case No. 1:25MJ29-1

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. 922(g)(1) | Possession of a firearm by a felon |
| 18 U.S.C. 922(o) | Possession of a machinegun |

The application is based on these facts:

See Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TREVOR MAYES Digitally signed by TREVOR MAYES Date: 2025.01.29 07:54:35 -05'00'

*Applicant's signature*

Trevor Mayes, Special Agent

*Printed name and title*

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 1/30/2025 3:09 pm

*Judge's signature*

City and state: Durham, North Carolina

Joe L. Webster, U.S. Magistrate Judge

*Printed name and title*

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH APPLE ID: kareemwarren602@icloud.com and kareemwarren0@icloud.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC. | Case No. 1:25MJ29-1 |

**AFFIDAVIT IN SUPPORT OF**
**AN APPLICATION FOR A SEARCH WARRANT**

I, Trevor S. Mayes, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Bureau of Alcohol, Tobacco, Firearm and Explosives ("ATF"), and have been since April 24, 2023. I am currently assigned to the Charlotte Field Division, Greensboro I Field Office. In my capacity as a Special Agent with the ATF, I have

received training related to criminal investigations to include crimes involving gang activity, firearms violations, drug trafficking, arson, explosives, money laundering, undercover operations, Title III wiretaps, as well as electronic and physical surveillance procedures. I have used my training to investigate violations of the Gun Control Act (GCA) and the National Firearms Act (NFA), such as firearms possession by prohibited persons, trafficking of firearms, machinegun manufacturing, etc. Before joining the ATF, I was employed as a Police Officer with the Pentagon Force Protection Agency (PFPA) since 2020. Within that role, I investigated violations and enforced laws according to United States Code (USC) and Virginia State Code.

3. I have a Bachelor of Science Degree in Criminal Justice from East Coast Polytechnic Institute (ECPI) Virginia Beach, VA. I am a graduate of the Federal Law Enforcement Training Center (FLETC) Uniformed Police Training Program (UPTP), Criminal Investigator Training Program (CITP), and the ATF Special Agent Basic Training program (SABT). The curriculum of these courses included training and instruction in Federal Criminal Law, Constitutional Law, Laws of Arrest, Laws of Evidence, Search and Seizure, Criminal Investigations.

4. The facts set forth in this affidavit are based upon my personal knowledge of this investigation, conversations with law enforcement officers and other individuals who have personal knowledge of the events and circumstances described herein, review of reports, documents, and recordings created by others, as well as information that I gained through training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(g)(1) [Possession of a Firearm by

Felon] and Title 18 U.S.C. § 922(o) [Possession of a Machine Gun] have been committed by Kareem WARREN. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

## JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## PROBABLE CAUSE

7. On December 3, 2023, at approximately 6:30 p.m., Officer Romps, with the Greensboro Police Department (GPD), was dispatched to the area of Highland Avenue and Barringer Street in reference to a wanted subject. Officer Romps reviewed the Computer-Aided Dispatch (CAD) notes, which advised that WARREN was at the corner of the intersection armed with a gun, and that WARREN was "on the run" from Ahoskie, NC. According to CAD, the 911 caller, hereinafter Woman-1, also reported that WARREN was wearing a cream- or light-colored hoodie and had dreads. Before arriving on scene, Officer Romps used a law enforcement database to verify WARREN had outstanding Orders for Arrest (OFA). Officer Romps arrived at the intersection Highland Avenue and Barringer Street at approximately 6:41pm to begin looking for WARREN.

8. Officer Brantley, who also responded to help locate WARREN, told Officer Romps that she observed an individual walking on Gregory Street, towards Barringer Street, wearing all light-colored clothing. Officer Romps responded to said location and saw WARREN walking on the road. Officer Romps parked her fully marked patrol vehicle, approached WARREN, and called

out to him to ask if he was Kareem. WARREN, with his hands in his pockets in front of him, turned and saw Officer Romps, and replied, "No." When WARREN turned, Officer Romps saw that WARREN had dreads and resembled the DMV photo she saw. After being ordered to stop, WARREN fled on foot.

9. While chasing WARREN, Officer Romps observed WARREN run to the right side of a residence, located at the 900 block of Barringer Street. Officer Romps heard a commotion behind the residence, but by the time she made it there, she lost sight of WARREN. Officer Romps observed a knocked over garbage can. She then heard footsteps on the fallen leaves in the backyard of the residence. Officer Romps then jumped the fence into the backyard when she heard Officer Brantley advise over the radio that she was chasing WARREN, who had rounded back to the front of the residence. WARREN ran across the street to the 1200 block of Gregory Street (approximately 100 feet), where WARREN was apprehended. It should be noted that the only time GPD officers lost sight of WARREN was when he ran behind the house on Barringer Street.

10. While WARREN was being searched for the firearm, he stated that he had lost his cell phone. No firearm was found on WARREN's person and WARREN denied tossing a firearm. When asked why he ran, WARREN replied "I don't know y'all." According to the CAD notes, at 6:46 p.m., Woman-1 told the 911 dispatcher that WARREN said the police were following him. Officer Romps then asked WARREN if he had a gun on him and he replied, "No, I didn't." Officer Romps then asked WARREN if he tossed a gun at the other house and he replied "No, of course not." When WARREN was being placed into the back of a patrol vehicle, he reiterated that he lost his cell phone.

11. Shortly after, Officer Huynh arrived on scene and deployed Canine Max along WARREN's flight path at the house on Barringer. Canine Max is trained to only locate and alert

on items that have a human odor on them. Canine Max alerted to a cell phone near two garbage cans on the right side of the house. It should be noted the cell phone still had power, which indicates that it hadn't been there for long. Also on the right side of the house is a chain-link fence that separates the front yard from the back yard. Shortly after, Canine Max alerted to a Polymer 80 firearm with no serial number and an extended magazine. The firearm was in the backyard, just on the other side of the fence, which is approximately 8 feet from the cell phone. The firearm was equipped with a Machine Gun Conversion Device (MCD), also known as a "switch." A MCD converts a semi-automatic firearm to a fully automatic firearm such that one pull of the trigger will expel multiple bullets. When the firearm was located, it appeared to be dry, although the surrounding leaves were wet from rain earlier in the day. Additionally, the firearm and cell phone were both found in WARREN's flight path.

12. WARREN was transported to the Guilford County Detention Facility for his state charges. The cellular phone that was recovered from behind the house on Barringer was given to the detention facility staff to be booked with WARREN's property. GPD Crime Scene Investigators (CSI) arrived and collected the Polymer 80 firearm for evidence. While GPD was still on scene, Corporal Walton spoke to the resident of the home on Barringer, Man-1. Man-1 stated that he heard a thud sound at the time WARREN was going behind his home.

13. On December 15, 2023, the National NIBIN [National Integrated Ballistic Information Network] Correlation and Training Center (NNCTC) developed several leads based on a correlation review of the test fire from the Polymer 80 firearm (recovered from Warren's flight path behind the home on Barringer Street on December 3, 2023) and ballistic evidence between cartridge casings recovered from the following: Williamston Police Department (WPD)

case 23-06-030 (Scene 1), GPD case 2023-1009-209 (Scene 2), and GPD case 2023-1118-138 (Scene 3).

14. Of particular note, Scene 2 occurred on October 9, 2023, just two months before the instant offense. The reports detailed a shooting in which an occupant of one vehicle and the driver of another vehicle exchanged gun fire. When the shooting occurred, a GPD officer was nearby in their patrol vehicle and they heard approximately 15 rapid shots that sounded as if they were being fired from a fully automatic weapon.

15. Scene 3 occurred on November 18, 2023 just a few weeks before the instant offense. According to the report, several GPD officers responded to apartment buildings in the 800 block of Rugby Street, Greensboro, NC, in reference to multiple residences and vehicles being struck by gunfire. An injured individual, Man-1, checked into Moses Cone hospital with a gunshot wound to the shoulder. Officers made contact with Man-1, who indicated he was on Rugby Street, but refused to answer any questions. Prior to police arriving on scene, CAD notes advised several different 911 callers reported seeing a group of people running and shooting at each other. Responding officers assessed property damage, looked for spent cartridge casings, and conducted witness interviews. One witness, Witness-1, reported that she was walking between buildings when she observed two groups of black males discharging firearms at one another. Many mixed caliber and brand cartridge casings were recovered from the scene.

16. There was also a small, concentrated area where multiple discharged Aguila brand 9mm casings were located near a tree in front of a home in the 800 block of Rugby Street. A witness, Witness -2, stated that a thin black male, wearing a blue sweatshirt frantically knocked on her door (which is attached to the house on Rugby St. where the casings were located) before facing away and firing at an unknown target. The Aguila 9mm casings showed a correlation with

the test fire from the Polymer 80 firearm that was recovered from Warren's flight path behind the residence located at the 900 block of Barringer Street on December 3, 2023.

17. On December 21, 2023, GPD Detective Clous seized WARREN's cell phone, with phone number ending in 5106, from the Guilford County Detention Facility, and provided a receipt for the seizure. On January 17, 2024, Detective Clous obtained a Search Warrant from a Guilford County Superior Court Judge for all AT&T records associated with the previously mentioned phone number. On January 24, 2024, Detective Clous received the records from AT&T. In particular, the records show WARREN's cell phone received a phone call at approximately 4:50pm from phone number ending in 9755 on the day of the shooting outlined above in paragraphs 15 and 16. The coordinates that the cell phone plotted to, as a result of that call, were 36.06112 latitude and -79.7749211 longitude. Detective Clous searched those coordinates in Google Maps, and determined that WARREN's phone was in an area near the intersection of Rugby Street and Decatur Street, which is approximately 500 feet from the residence on Rugby Street where the casings were located in Scene 3 described in paragraphs 15 and 16. The location data of WARREN's cell phone indicate that his phone was in the area of the shooting during the time it happened and, as stated above, the casings recovered from that shooting were determined to be fired from the Polymer80 recovered when Warren was arrested in December 2023. [Agent note: after talking to Detective Clous, I learned the subscriber of the phone number ending in 5106, was

another individual who was incarcerated during the time of the shooting. As such, that individual could not have been at the scene of the shooting on November 18, 2023.]

18. On June 27, 2024, Firearm and Toolmark Examiner Lendel-Hardin completed a Firearms Examination Report. The report determined the previously mentioned Polymer 80 firearm is capable of firing fully automatic.

19. On October 24, 2024 I listened to some of WARREN's jail calls. On one jail call, placed on December 4, 2023, at 2:46 p.m., WARREN called Woman-1. WARREN inquired about his iPhone and his "bread," then told Woman-1 to take those items to "the room" and give it to an unknown third party. In the same call, WARREN expressed his anger with Woman-1 and accused her of getting him locked up. On the same day, at 2:49 p.m., WARREN called a phone number ending in 1061 and spoke to an unknown male. WARREN told the unknown male that Woman-1 is bringing his iPhone to "the room." The phone recovered from behind the residence on Barringer Street during WARREN's December 3, 2023, arrest is an Android brand phone. As such, WARREN's statements on the jail calls indicate that he also has an iPhone that was not recovered by GPD. Based on my experience and conversations with colleagues, it is common for individuals involved in criminal activity to have two phones, one phone being their main phone and the other one being cheap and easy to dispose of (i.e. a burner phone). Based on my training and experience

20. On October 25, 2024, SA Elijah Carpenter and I conducted a custodial interview of WARREN while he was in custody at the High Point Detention Facility. WARREN was in custody for his state firearm and drug charges. I read WARREN his Miranda Rights, which he waived and agreed to answer questions. I asked WARREN about his Greensboro arrest on December 3, 2023. WARREN said he was coming from his girlfriend's house, and he didn't know that it was the police that was trying to stop him. WARREN then said he ran behind a house and ran into a trash

can then hopped a fence before he was apprehended a short distance later. WARREN confirmed the police got his phone because he had it in his hand as he was running and dropped it. WARREN confirmed he knows who Woman-1 is (the 911 caller). I then inquired about WARREN's knowledge of "switches." WARREN stated that a switch makes a gun shoot from semi-automatic to fully automatic.

21. I then asked WARREN about the November 18, 2023, shooting in Greensboro. WARREN denied any involvement and seemingly became agitated when I brought up evidence. WARREN also talked about how he was shot in 2019, and as a result, he takes unprescribed pills, such as Percocet, to help with the pain.

22. On October 28, 2024, I conducted a telephonic interview with Woman-1. Woman-1 said due to an upcoming funeral, she was unable to meet in person. I asked Woman-1 to talk about what led up to her calling 911 on WARREN on December 3, 2023. Woman-1 said she was giving WARREN a ride when her and WARREN began arguing. Woman-1 said she became angry when WARREN called her a bunch of bad names, so she told WARREN to get out of her car. Woman-1 said she then called 911 because she knew WARREN had warrants. Lastly, Woman-1 said before WARREN got out of her car, she saw that WARREN had a pistol in his lap.

23. On November 20, 2024, I served a subpoena to Apple Inc. to identify an Apple ID for WARREN. On November 25, 2024, I received the records from said subpoena. Upon reviewing these records, I was able to identify WARREN's Apple ID as kareemwarren602@icloud.com. Apple indicated that the Apple ID was created on September 16, 2023. The address associated with the account is 903 1st Street East, Ahoskie, NC 27910. This is a known address for WARREN. The phone number verified for the account is ***-***-7133. I was able to determine from these records that WARREN is currently utilizing the iCloud for the

following features: Calendars, Bookmarks, iCloud Photos, Contacts, iCloud Drive, iCloud Reminders, Mail, Mail Header, and Notes.

24. Additionally, WARREN has another active Apple ID, kareemwarren0@icloud.com, which was created on November 9, 2020, with the same Ahoskie, NC address. The phone number verified for the account is ***-***-4129. I was able to determine from these records that WARREN is currently utilizing the iCloud for the following features: Calendars, Bookmarks, iCloud Photos, Contacts, iCloud Drive, Mail, Mail Header, and Notes.

25. Based on my training and experience, I know that it is common for persons involved in criminal activity to use their cellular smartphone device to communicate with other involved associates prior to, during and after the commission of a crime. Frequently persons involved in criminal activity often glorify, boast and publicize their illegal activities including their weapons, for many reasons including notoriety and the intimidation of others. This is done through pictures, video, multimedia, text messages, and incoming and outgoing phone calls and the vast variety of mobile applications available and accessed directly through the smartphone device. Modern smartphones and their storage systems, such as Apple iCloud, are of great value for both lawful and unlawful purposes as they are an insistent part of daily life.

26. Furthermore, it is common for individuals to use their cellular smartphones to access the internet. Access to the internet via a cellular device typically creates a log of items which are viewed and searched on the internet and as such, creates a recorded history. It is further known that this history is rarely completely deleted. A variety of third-party software components called "apps," are reliant on internet access for their functionality. Popular and commonly used apps such as Facebook, Instagram, and Twitter offer a range of tools for managing detailed information about all aspects of a person's life though installation, storage and use of the device.

## BACKGROUND CONCERNING APPLE[1]

27. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

28. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased

through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

29. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

30. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

31. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

32. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

33. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email

(iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

34. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

35. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

36. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

37. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

39. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including

information that can be used to identify the account's user or users. Based upon WARREN's proven utilization of electronic devices to facilitate his criminal activities, I believe that the records maintained by Apple will likely contain images, videos, text messages, call logs, and other evidence which are indicative of the sale and distribution of firearms and controlled substances.

## CONCLUSION

40. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that that violations of 18 U.S.C. § 922(g)(1) [Possession of a Firearm by Felon] and Title 18 U.S.C. § 922(o) [Possession of a Machine Gun] have been committed by Kareem WARREN. There is probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

41. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant authorizing the search and seizure of information associated with the account described in Attachment A, and to seek items described in Attachment B.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Trevor S. Mayes

Trevor S. Mayes

ATF Special Agent
Bureau of Alcohol, Tobacco, Firearms &
Explosives

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 30th day of January, 2025, at 3:09 p.m.

Honorable Joe L. Webster
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

### Property to Be Searched

This warrant applies to information associated with APPLE ID: kareemwarren602@icloud.com and kareemwarren0@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

## ATTACHMENT B

### Particular Things to be Seized

### I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account from **June 1, 2023 to present**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from **June 1, 2023 to present**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of the SUBJECT OFFENSE involving Kareem WARREN and occurring after **June 1, 2023,** including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a) The illegal possession, manufacture, distribution, and sale of firearms

b) All records, information and communications relating to communication or contact between Kareem WARREN and individuals involved in the commission of the crimes under investigation;

c) The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

d) Evidence indicating how and when the account was accessed or used;

e) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

f) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts;

g) Images depicting the interior or exterior of residences, public establishments, and vehicles relating to the crime under investigation;

h) All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

i) All images, messages, and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

j) Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A;

k) All existing printouts from original storage which concern the categories identified in subsection II; and

l) All "address books" or other lists of contacts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.